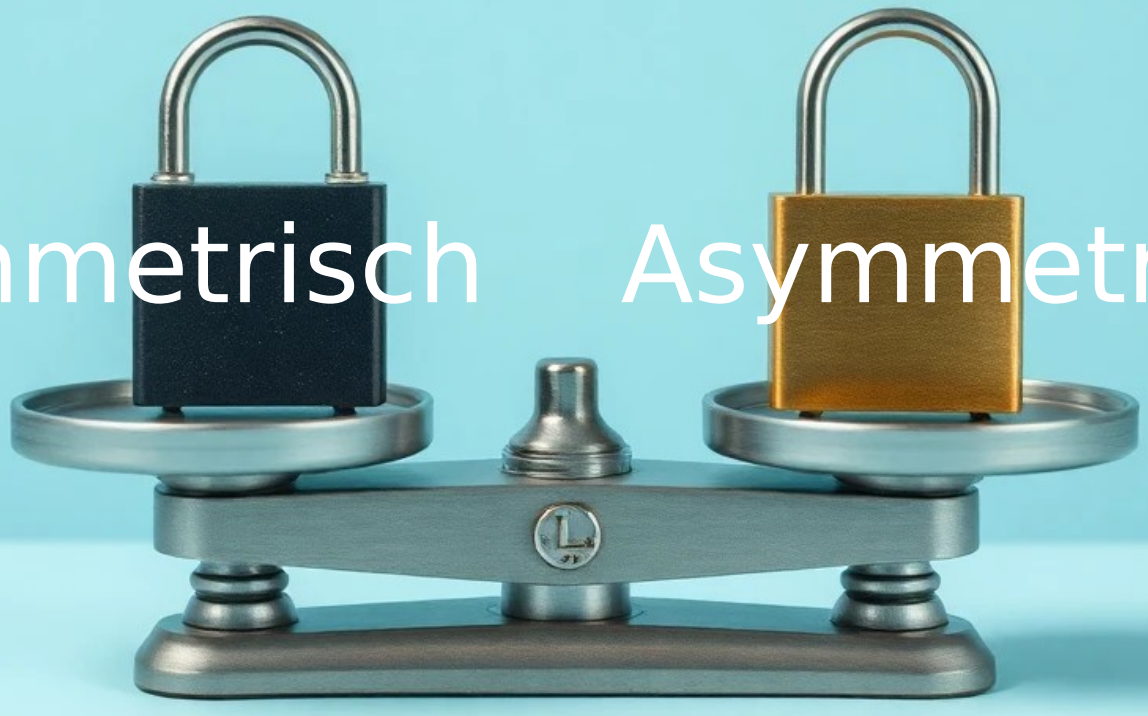
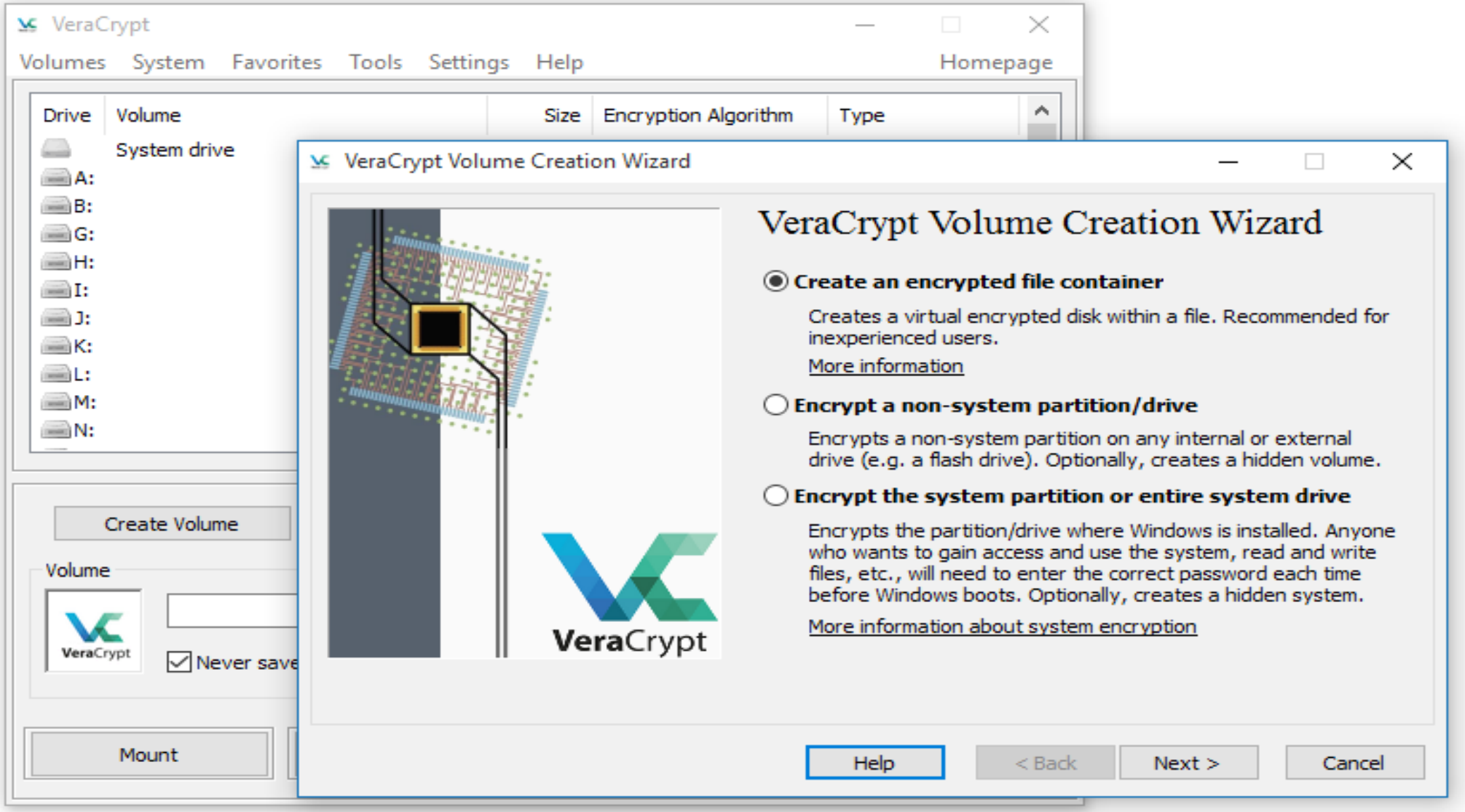
Verschlüsselungsalgorithmen

Symmetrisch Asymmetrisch



und VeraCrypt


VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
System drive
A:
B:
G:
H:
I:
J:
K:
L:
M:
N:
Create Volume
Volume
VeraCrypt
Never save
Mount
VeraCrypt Volume Creation Wizard
VeraCrypt Volume Creation Wizard
Create an encrypted file container
Creates a virtual encrypted disk within a file. Recommended for inexperienced users.
More information
Encrypt a non-system partition/drive
Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.
Encrypt the system partition or entire system drive
Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.
More information about system encryption
VeraCrypt
Help
< Back
Next >
Cancel

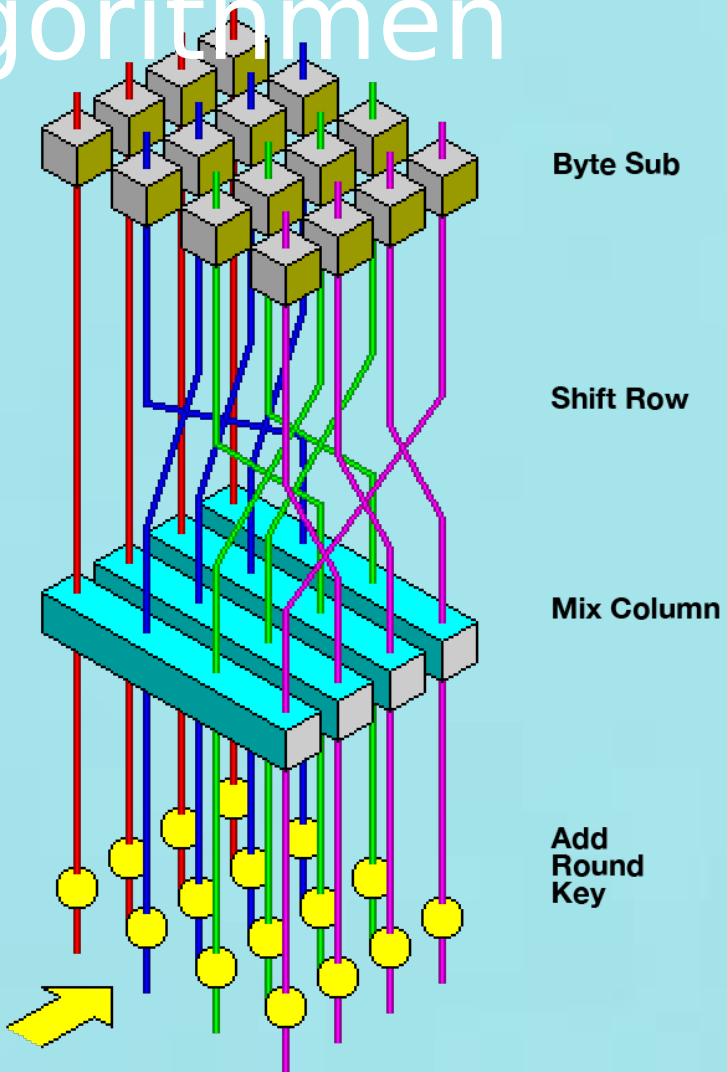
Einleitung

- Freie Software mit offenem Quellcode zur Datenverschlüsselung.
- Verschlüsselt Dateien, Partitionen oder ganze Speichermedien.
- Nutzt starke Verfahren wie AES, Serpent und Twofish (kombinierbar).
- Verfügbar für Windows, macOS, Linux (systemübergreifend).
- 11 Jahre Entwicklungszeit und

VeraCrypt

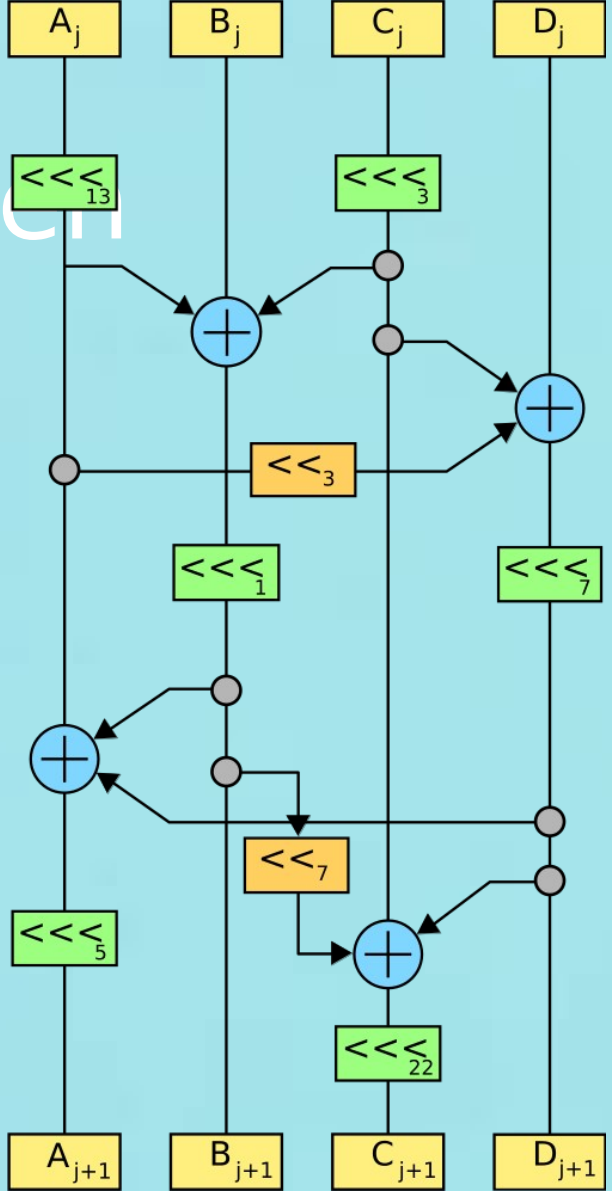
Tiefer in die Verschlüsselungsalgorithmen

- **AES (Advanced Encryption Standard):**
  - Schnellster Algorithmus mit 14 Runden.
  - Nutzt mathematische Operationen im Galois-Feld GF(2^8).
  - Hardwarebeschleunigung (AES-NI) für maximale Geschwindigkeit.
  - Ideal für Echtzeitanwendungen (Festplatten, HTTPS).
  - Unterstützt Schlüssel bis 256 Bit.



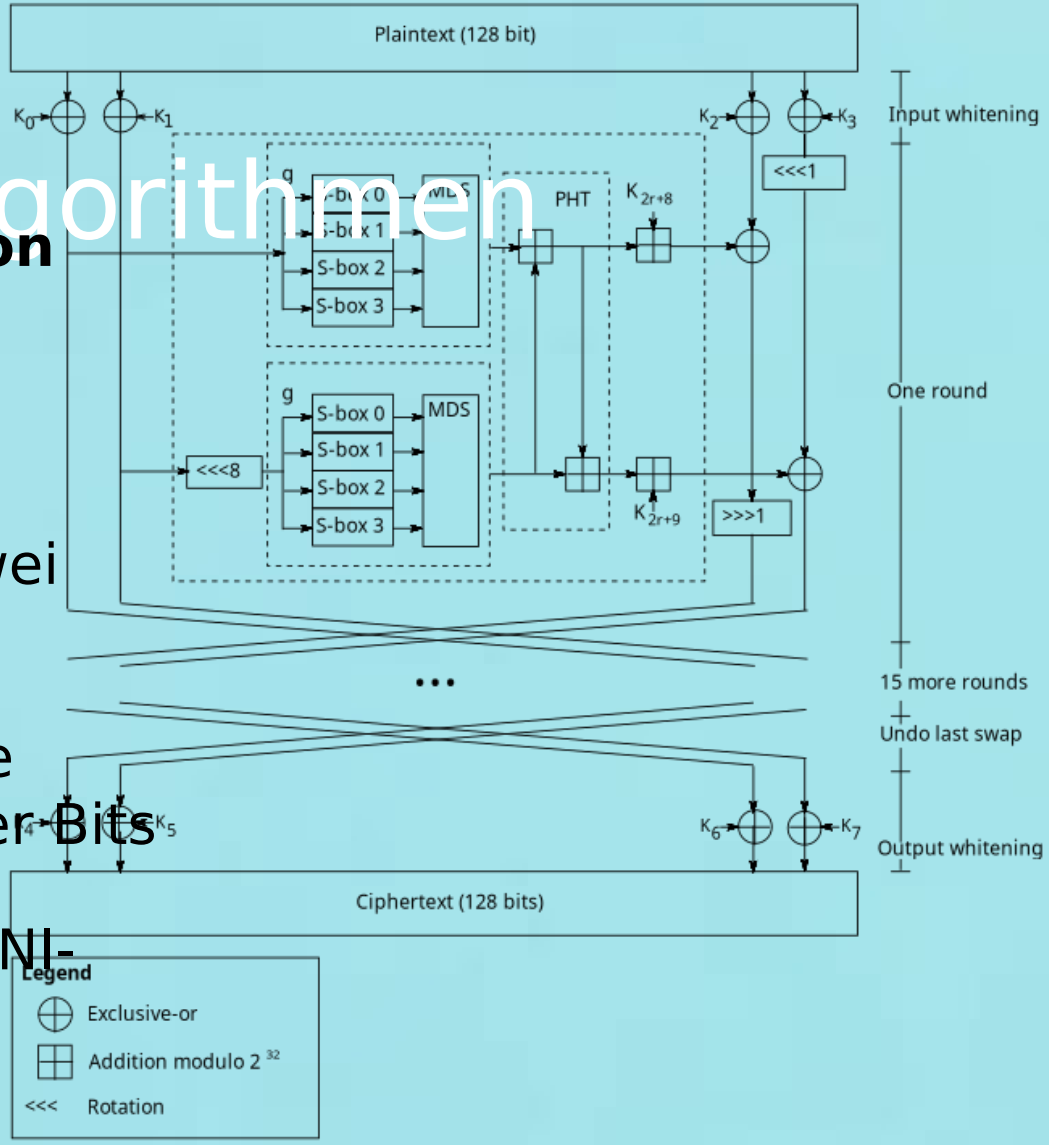
Tiefer in die Verschlüsselungsalgorithmen

- **Serpent (engl. für Schlange):**
  - 32 Runden (mehr als AES/Twofish).
  - Einfache Bitoperationen (XOR, Schiebeoperationen, lineare Transformation, S-Boxen).
  - Resistent gegen Quantencomputer.
  - Langsam, aber extrem sicher.
  - Generiert 132 Rundenschlüssel aus Hauptschlüssel
  - Keine CPU-Befehle, die die Algorithmusleistung beschleunigen



Tiefer in die Verschlüsselungsalgorithmen

- **Twofish (die "zweite Version" von Blowfish):**
  - Runden: 16
  - Feistel-Netzwerk: Teilt Daten in zwei Hälften für parallele Verarbeitung.
  - MDS-Matrizen (Maximum Distance Separable): Maximale Diffusion der Bits
  - übertrifft AES auf CPUs ohne AES-NI-Beschleunigung dank effizienter Softwareoptimierung.
  - 40 Rundenschlüssel (16 Runden ×



Mehr zur Geschwindigkeit

- **AES-NI-Befehle (Advanced Encryption Standard New Instructions)**
  - wurden von Intel im Jahr 2010 mit der Westmere-Architektur (z. B. Core i5/i7) eingeführt.
  - AMD folgte später zwischen 2011–2012 mit der Bulldozer-Architektur.
- **Twofish**
  - Code ist effizient für 32/64-Bit-CPUs geschrieben.
  - Teilt Daten in zwei Hälften, die unabhängig verarbeitet werden können → ideal für Multithreading.
- **Serpent**
  - Immer langsam

- Die Galois-Felder (Galois-Fields) wurden endgültig im Jahr **1846** veröffentlicht.

- **1971**: Das Geburtsjahr des Feistel-Netzwerks.

- **1975** wurde der Data Encryption Standard (DES) als FIPS 46 vom National Bureau of Standards (NBS) offiziell standardisiert.

- Der AES-Wettbewerb begann am 2. Januar **1997** und läutete eine neue Ära der Kryptografie ein.

- Am 15. Juni **1998** endete die Einreichungsfrist für Algorithmen im AES-Wettbewerb.

Evariste

Quellen

Bilder

e 1: https://web.archive.org/web/20250421174542/https://page-images.websim.ai/two_locks_on_the_pans_of_a_balance_scale_ac5cd1cd91ca
e 3: https://upload.wikimedia.org/wikipedia/commons/thumb/6/6a/VeraCrypt_Logo.svg/2497px-VeraCrypt_Logo.svg.png
e 4: https://upload.wikimedia.org/wikipedia/commons/thumb/6/6a/VeraCrypt_Logo.svg/2497px-VeraCrypt_Logo.svg.png
e 5: https://en.wikipedia.org/wiki/File:Serpent-linearfunction.svg
e 6: https://upload.wikimedia.org/wikipedia/commons/e/ee/Twofishalgo.svg
e 8: https://upload.wikimedia.org/wikipedia/commons/5/53/Evariste_galois.jpg
e 2: https://upload.wikimedia.org/wikipedia/commons/8/80/VeraCrypt_screenshot.png

Text

https://en.wikipedia.org/wiki/Serpent_(cipher)
http://embeddedsw.net/Cipher_Reference_Home.html#SERPENT
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
https://web.archive.org/web/20160306104007/http://research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf
https://en.wikipedia.org/wiki/VeraCrypt
https://github.com/veracrypt/VeraCrypt
https://en.wikipedia.org/wiki/Twofish
https://www.schneier.com/paper-aes-comparison.html
https://de.wikipedia.org/wiki/Endlicher_K%C3%B6rper
https://archive.org/details/historyabstracta00klei_911
https://nvlpubs.nist.gov/nistpubs/sp958-lide/250-253.pdf
https://en.wikipedia.org/wiki/Data_Encryption_Standard